

Claims

What is claimed is:

- 1 1. A method for charging a smart battery, the method comprising:
2 receiving an encrypted random string, wherein the encrypted random
3 string includes a random string in an encrypted form;
4 decrypting the encrypted random string to recover the random string;
5 and
6 transferring the random string to a device to authenticate the smart
7 battery for the charging, the device being electrically coupled to the smart
8 battery.

- 1 2. The method of claim 1, wherein the receiving comprises:
2 generating a random string, the random string being generated by the
3 device;
4 encrypting the random string, the random string being encrypted with
5 an encryption key included in the device to generate the encrypted random
6 string;
7 transferring the encrypted random string, the encrypted random string
8 being transferred from the device to the smart battery.

- 1 3. The method of claim 2, wherein the decrypting requires the encryption key.

- 1 4. The method of claim 2, wherein the encryption key is a private key.

- 1 5. The method of claim 2, wherein the encrypted form is defined by the device
2 and includes the encryption key to encrypt the random string.

- 1 6. The method of claim 2, wherein the encryption key is at least 8 bits.
- 1 7. The method of claim 2, wherein the generating, encrypting and transferring is
2 performed by a controller included in the device, wherein the device is
3 included in an information handling system.
- 1 8. The method of claim 1, wherein the device authenticates the smart battery by
2 verifying the random string is unchanged.
- 1 9. The method of claim 8, wherein the device identifies the smart battery as a
2 counterfeit when the random string is changed, wherein the device disables
3 the charging of the counterfeit.
- 1 10. The method of claim 1, wherein the encrypted form is defined by the device
2 and includes an encryption key to encrypt the random string.
- 1 11. The method of claim 1, wherein the random string is alpha numeric.
- 1 12. The method of claim 1, wherein the random string is a random number.
- 1 13. The method of claim 1, wherein the transferring of the random string is via an
2 SMBus.

- 1 14. A method for authenticating a smart battery, the method comprising:
2 generating a first random string, the first random string being
3 generated by a device electrically coupled to the smart battery;
4 encrypting the first random string, the first random string being
5 encrypted with a first encryption key included in the device to generate the
6 encrypted first random string;
7 transferring the encrypted first random string, the encrypted first
8 random string being transferred from the device to the smart battery;
9 decrypting the encrypted first random string with the first encryption
10 key to recover a second random string;
11 encrypting the second random string, the second random string being
12 encrypted with a second encryption key included in the smart battery to
13 generate the encrypted second random string;
14 transferring the encrypted second random string, the encrypted
15 second random string being transferred from the smart battery to the device;
16 decrypting the encrypted second random string with the second
17 encryption key to recover the second random string; and
18 verifying the first random string and the second random string match to
19 authenticate the smart battery.
- 1 15. The method of claim 14, wherein each of the first and second encryption keys
2 is a private key.
- 1 16. The method of claim 14, wherein each of the first and second encryption keys
2 is at least 8 bits.
- 1 17. The method of claim 14, wherein each of the first and second random strings
2 is a random number.

- 1 18. A smart battery authentication system comprising:
2 a smart battery, wherein the smart battery includes:
3 a smart electronics operable to:
4 receive an encrypted random string, wherein the
5 encrypted random string includes a random string in an
6 encrypted form;
7 decrypt the encrypted random string to recover the
8 random string; and
9 transfer the random string to a controller to authenticate
10 the smart battery;
11 a communications bus for electrically coupling the smart
12 electronics to the controller; and
13 the controller operable to authenticate the smart battery by
14 generating the random string, generating the encrypted random string
15 and verifying the random string is unchanged.
- 1 19. The system of claim 18, wherein the encrypted form is defined by the
2 controller and includes an encryption key to encrypt the random string.
- 1 20. The system of claim 18, wherein the random string is a random number.

- 1 21. An information handling system comprising:
2 a processor;
3 a system bus;
4 a memory coupled to the processor through the system bus;
5 a power supply system operable to provide power to the processor, the
6 bus and the memory, the power supply system being connectable to an AC
7 adapter for deriving power from an AC power source;
8 a controller coupled to the processor and memory through the system
9 bus, the controller operable to control the power supply system; and
10 wherein the power supply system includes:
11 a smart battery having a smart electronics, the smart electronics
12 being operable to:
13 receive an encrypted random string, wherein the
14 encrypted random string includes a random string in an
15 encrypted form;
16 decrypt the encrypted random string to recover the
17 random string; and
18 transfer the random string to the controller to
19 authenticate the smart battery.
- 1 22. The system of claim 21, wherein the controller is operable to authenticate the
2 smart battery by generating the random string, generating the encrypted
3 random string and verifying the random string is unchanged.